



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/808,720	03/15/2001	Hakon Gudbjartsson	2345.2003-001	5511
21005	7590	06/29/2007	EXAMINER	
HAMILTON, BROOK, SMITH & REYNOLDS, P.C. 530 VIRGINIA ROAD P.O. BOX 9133 CONCORD, MA 01742-9133			KLIMACH, PAULA W	
		ART UNIT	PAPER NUMBER	
		2135		
		MAIL DATE	DELIVERY MODE	
		06/29/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	09/808,720	GUDBJARTSSON ET AL.
	Examiner	Art Unit
	Paula W. Klimach	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 05 April 2007.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1,2,4,7-21,23 and 25-41 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-2, 4, 7-21, 23, and 25-41 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 04/05/07. The amendment filed on 04/05/07 have been entered and made of record. Therefore, presently pending claims are 1-2, 4, 7-21, 23, 25-41.

Response to Arguments

Applicant's arguments filed 04/05/07 have been fully considered.

Applicant argued that Challener does not disclose or suggest a method having the anonymous, one-to-one mapping, as amended, because Challener does not teach the reversible mapping. This is not found persuasive. The applicant does not claim reversible mapping. The one-to-one mapping shown in Challener is the mapping of the voter information with the mapping of the id to the vote.

The applicant argued further that Mital, Shamir, and Schneier do not disclose one-to-one mapping. This is found persuasive because Challener teaches this limitation.

The applicant argues further that Mital and Shamir do not suggest or teach authenticating with a communications module. This is persuasive because Schneier teaches this limitation.

The applicant argues further that Schneier does not teach two parties authenticate each other with the communication module. This is not found persuasive. In the Dass protocol, Schneier teaches Alice and Bob authenticating using Trent, wherein Alice corresponds to the sender, Bob corresponds to the receiver, and Trent corresponds to the communication module.

Due to the arguments provided above, the rejection of the independent, provided below, claims is maintained. The dependent claims are rejected at least by their dependence on the independent claims and further for the reasons given below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-2, 7-8, 16-19, 20-21, 25-30, 34-37, and 40-41 are rejected under 35 U.S.C.

103(a) as being unpatentable over Challener (6,081,793) in view of Mital (5,903,652) and further in of the article by Shamir ("How to Share a Secret") and further in view of the book by Schneier ("Applied Cryptography").

In reference to claims 1 and 20. a communication module for establishing a communication connection between a sender of one working data identifier set domain and a receiver in a different working data identifier set domain (Fig. 1); a mapping module coupled to the communication module for anonymously mapping working data of the one working data identifier set domain to working data of the different working data identifier set domain, the working data having (i) a research data portion and (ii) an identifier portion related to identifying persons associated with the research data portion (column 7 lines 1-37), the mapping module mapping the identifier portion of the working data in the one working data identifier set domain to the identifier portion of the working data in the different working data identifier set domain

such that the working data transmitted to the authorized receiver is anonymous data, while leaving the research data portion unmapped by the anonymous mapping of the identifier portions (authentication server Fig. 7 and column 7 lines 50-67); and a secret sharing module for performing secret sharing to control key holder access to the mapping module (parts 379, 391, 439 Fig. 7); the apparatus communicating between parties comprising at least the sender (part 225 Fig. 1A) and the receiver (part 229 Fig. 1A) in at least two different working data identifier set domains (column 7 lines 38-67 in combination with column 8 lines 45-52).

The applicant does not define working data identifier set domain. The definition of working data identifier set domain is data that devices process that are divided into sets. Although Challener does not describe that data that is processed by the authentication server and the results server as working data identifier set domain, the data sets that the authenticator and the results server process are different sets of data. The authenticator processes that identification data and the results server processes that ballot.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to describe the data processed by the authentication server and the results server of Challener as working data identifier sets. One of ordinary skill in the art would have been motivated to do this because the data revealed to the different servers in system of Challener is separated by encryption so that the voter cannot be identified from their ballot (column 10 line 51-67).

Although Challener discloses transmitting anonymously mapped identifier portion and the unmapped research data portion of the working data to the receiver, the mapping module of

Challener is not capable of accessing both the identifier portion and the research data portion of the working data.

Mital discloses a system wherein the communication module is capable of transmitting both the anonymously mapped identifier portion and the unmapped research data portion of the working data to the receiver (column 7 line 65 column 8 line 14). The system of Mital further discloses that the mapping module is capable of accessing both the identifier portion and the research data portion of the working data (column 27 lines 54-61).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to make the mapping module capable of accessing both the identifier portion and the research data portion of the working data as in Mital and therefore allowing the viewing of data, but disallowing access using encryption in the system of Challener. One of ordinary skill in the art would have been motivated to do this because it would provide access to portions of information that are required by specific users while denying access by use of encryption to data that requires hiding from certain users.

Although Challener teaches encryption and therefore the use of keys, Challener does not disclose a predetermined number of keyholders greater than one is required to compromise access to the mapping module.

Shamir teaches a hot to divide data into n pieces in such a way that the data is easily reconstructable from any k pieces, but even complete knowledge of k-1 pieces reveals absolutely no information about D (abstract). The method is an efficient threshold scheme for the management of keys. Therefore Shamir teaches a method for sharing a predetermined number of

keyholders greater than one is required to compromise access to the mapping module (page 612).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to divide the key into different shares for multiple key holders as in the process taught by Shamir in the system of Challener. One of ordinary skill in the art would have been motivated to do this because the scheme is ideally suited to application in which a group of mutually suspicious individuals with conflicting interests must cooperate (Shamir page 612).

Challener does not disclose a mutual authentication system wherein the communication connection is a secure communication channel formed by the communication module (i) authenticating the sender and receiver, resulting in an authorized sender and authorized receiver, and (ii) encrypting working data transmitted over the channel.

In reference to claims 2 and 21, a system is disclosed wherein the research data portion of the working data includes personal data of individuals (column 7 lines 1-10 and 55-60).

In reference to claims 7 and 25, Challener discloses permanent storage means for storing data in a tamper-proof manner (Fig. 1C and Fig. 7).

In reference to claims 8 and 26, wherein the permanent storage means encrypts non-queried parts of the data, said encryption using an encryption key, and the secret sharing module storing the encryption key (part 377 Fig. 7).

In reference to claims 16 and 34, wherein connection of the sender and receiver are respectively one of a software implementation and a human being.

Although Challener discloses the sender being a software implementation (authentication server has software running on it), Challener does not disclose the receiver being a human being

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send the ballots of Challener to a human being. One of ordinary skill in the art would have been motivated to do this because the human being would have interest in the results of the ballot for voting purposes.

In reference to claims 17 and 35, wherein connection of the sender and receiver is in respective different sessions.

Although Challener discloses the sender and the receiver viewing different forms of the information, Challener does not expressly disclose the sender and the receiver connection is in respectively different sessions

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to connect the receiver and sender in different session. One of ordinary skill in the art would have been motivated to do this because the receiver is interested in the result of the ballot and therefore connection of the receiver is advantages after the voting has occurred and therefore in a separate session.

In reference to claims 18 and 36, wherein the communication module further enables communication connection by a supervisor in addition to the sender and receiver (part 227 Fig. 1A).

In reference to claims 19 and 37 wherein the communication connection by the supervisor enables remote operation of the apparatus by the supervisor (Fig. 1C).

In reference to claims 40-41 wherein the working data is formed of plural records, each record comprising (i) a research data portion and (ii) an identifier portion related to identifying .

Art Unit: 2135

an individual person associated with the research data portion, the individual person being the same person across each record of the plural records.

The vote of Challener can be increased to include more data. Therefore At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to increase the data provided in the section for the vote. One of ordinary skill in the art would have been motivated to do this because the amount of data required by a system depends on the type of system.

Claims 4, 9-12, 23, 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener and further in view of Mital and Shamir and Stallings as applied to claims 1 and 20 above, and further in view of Schneier.

In reference to claim 4 and 23, a system is disclosed wherein the mapping module employs encryption in the mapping of working data in the domain to working data in the different domain such that the working data transmitted to the authorized receiver is anonymous data (column 6 lines 14-59).

In reference to claims 9 and 27, Challener does not expressly disclose a system wherein the permanent storage means employs digital signatures on queried parts of the data to detect changes in data and thereby prevent tampering.

Schneier discloses a system of blind signatures where the document is signed and the person does not know what they are signing (pages 112-114). Digital signatures are used to detect changes in the data.

Art Unit: 2135

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use blind signatures as in Schneier in the system of Challener. One of ordinary skill in the art would have been motivated to do this because the person that signed the document can verify that they signed it, but will not know the contents of the document.

In reference to claims 10 and 28, Challener discloses the concatenation of the encryption key and data (column 5 lines 42-54), however Challener does not disclose digital signature is formed from a message digest.

Schneier discloses generating a message digest using a one-way hash and then signing the message digest (pages 38-39).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to sign a message digest as in Schneier in the system of Challener. One of ordinary skill in the art would have been motivated to do this because it increases the speed of signing documents.

In reference to claims 11 and 29, Challener does not disclose a system wherein the permanent storage means maintains a summary measure of stored data

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a summary measure of stored data in the system of Challener. One of ordinary skill in the art would have been motivated to do this because it enable the reconstruction of data in the case of corruption of the original.

In reference to claims 12 and 30, Challener does not disclose a system wherein said summary measure has a respective digital signature.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a summary measure of stored data that has a digital signature in the system of Challener. One of ordinary skill in the art would have been motivated to do this because it would enable the detection of changes to the summary measure.

Claims 13-15, 31-33, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener and further in view of Mital and Shamir and Stallings as applied to claims 1 and 20 above, and further in view of Ansell et al (6,151,631).

In reference to claims 13 and 31, Challener does not expressly disclose storing a mapping table having cross-references between identifier portions of working data of the two domains

However Ansell discloses storing a mapping table (fig. 13 part 1306), the mapping table having cross-references between identifier portions of data of different domains (fig. 13 parts 1302 and 1304)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain mapping tables as in Ansell in the system of Challener. One of ordinary skill in the art would have been motivated to do this because a mapping table organizes the information in a convenient manner.

In reference to claims 14, 32, and 38, Challener does not disclose a system wherein the mapping module stores a mapping table for plural domains, the mapping table being formed of (i) an index section and (ii) a working reference section, the index section indicating identifier portion of working data in a first subject domain and the working reference section indicating corresponding identifier portion in a second domain, the working reference being encrypted,

such that the mapping module performs decryption on a part of the mapping table to determine usable cross reference of the working data.

However Ansell discloses a system wherein the mapping module stores a mapping table for plural domains (Fig. 13 part 1306), the mapping table being formed of (i) an index section and (ii) a working reference section, the index section indicating identifier portion of working data in a first subject domain and the working reference section indicating corresponding identifier portion in a second domain, the working reference being encrypted, such that the mapping module performs decryption on a part of the mapping table to determine usable cross reference of the working data (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain mapping tables as in Ansell in the system of Challener. One of ordinary skill in the art would have been motivated to do this because a mapping table organizes the information in a convenient manner.

In reference to claims 15 and 33, Challener does not disclose a system wherein the mapping module maps working data among plural domains.

Ansell disclose a system wherein the mapping module maps working data among plural domains (Fig. 13 part 1306).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain mapping tables as in Ansell in the system of Challener. One of ordinary skill in the art would have been motivated to do this because a mapping table organizes the information in a convenient manner.

Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Challener in view of Mital in view of the article by Shamir and further in view of Schneier as applied to claim 1 above, and further in view of Coss et al (EP 0 909 074 A1).

Challener discloses a system with a secure container (part 30 in Fig. 1); a computer system executing the communication module and the mapping module (part 30 in Fig. 1).

However Challener does not disclose a firewall coupled to the computer system, the firewall being housed by the secured container so as to provide tamper-proof hardware.

Coss discloses a system with a firewall with the capability for supporting multiple domains (Page 4 paragraph 0025). Firewalls include tamper-proof hardware by definition.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to include a firewall capable of supporting multiple domains as in Coss in the system of Challener. One of ordinary skill in the art would have been motivated to do this because firewalls prevent unauthorized access in computer networks.

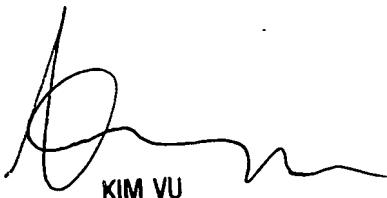
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, June 25, 2007



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100